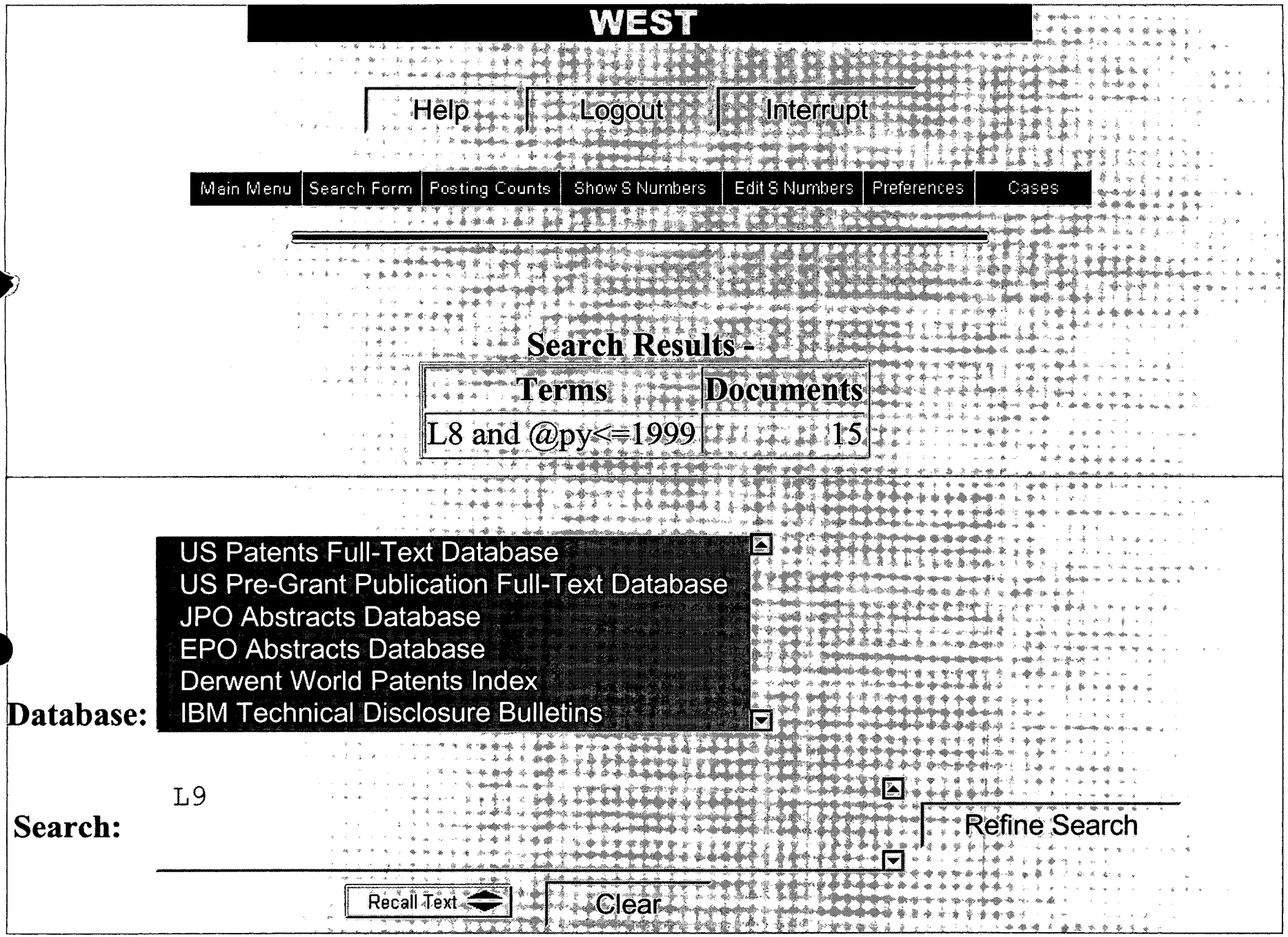
WEST
Help
Logout
Interrupt
Main Menu
Search Form
Posting Counts
Show S Numbers
Edit S Numbers
Preferences
Cases
Search Results -
Terms
Documents
L8 and @py<=1999
15
US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins
Database:
L9
Search:
Refine Search
Recall Text
Clear

Search History

DATE: Friday, March 08, 2002 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=OR		
L9	L8 and @py<=1999	15	L9
L8	(transmit$ or transfer$ convey$) near15 (first network$) near15 (authorizat$ or authenticat$) near19 (pay$) near19 (second network$) near18 (packet$ data$)	31	L8
L7	L6 and (payment$)	14	L7
L6	l1 and @py<=1999	195	L6
L5	l1 and @py<=1999 and ((705/1 |705/2 |705/3 |705/4 |705/5 |705/6 |705/7 |705/8 |705/9 |705/10 |705/11 |705/12 |705/13 |705/14 |705/15 |705/16 |705/17 |705/18 |705/19 |705/20 |705/21 |705/22 |705/23 |705/24 |705/25 |705/26 |705/27 |705/28 |705/29 |705/30 |705/31 |705/32 |705/33 |705/34 |705/35 |705/36 |705/37 |705/38 |705/39 |705/40 |705/41 |705/42 |705/43 |705/44 |705/45 |705/400)!.CCLS.)	6	L5

Reviewed all of L9

Reviewed titles of L6

Considered

L4	(first network$) near17 (authoriz$ or authenticat$) near19 (packet$) near19 (second network$)	374	L4
L3	l1 and L2 and @py<=1999 and ((705/1 |705/2 |705/3 |705/4 |705/5 |705/6 |705/7 |705/8 |705/9 |705/10 |705/11 |705/12 |705/13 |705/14 |705/15 |705/16 |705/17 |705/18 |705/19 |705/20 |705/21 |705/22 |705/23 |705/24 |705/25 |705/26 |705/27 |705/28 |705/29 |705/30 |705/31 |705/32 |705/33 |705/34 |705/35 |705/36 |705/37 |705/38 |705/39 |705/40 |705/41 |705/42 |705/43 |705/44 |705/45 |705/400)!.CCLS.)	1	L3
L2	(transmit$ or convey$) near15 (first network$) near15 (second network$) near15 (pay$)	599	L2
L1	(first network$) near17 (authoriz$ or authenticat$) near19 (packet$) near19 (second network$)	374	L1

END OF SEARCH HISTORY

End of Result Set

L3: Entry 1 of 1 File: USPT Mar 3, 1998

DOCUMENT-IDENTIFIER: US 5724424 A
TITLE: Digital active advertising

YEAR ISSUED (ORACLE) (1):
1998

Current US Cross Reference Classification (3):
705/26

CLAIMS:

1. An open network sales system providing for real-time authorization of purchase transactions, comprising:

a plurality of buyer computers; and

a plurality of merchant computers;

said plurality of buyer computers and said plurality of merchant computers being interconnected by a public packet switched communications network;

at least one of said plurality of merchant computers being programmed to store digital advertisements in a database;

each one of said buyer computers being programmed to receive a user inquiry and, in response to said user inquiry, to select at least one of said merchant computers and to transmit a network request thereto over said public packet switched communications network;

at least one of said merchant computers being programmed to cause one of said digital advertisements to be communicated to said one of said buyer computers over said public packet switched communications network in

response to said network request from said buyer computer;

said one of said buyer computers being programmed to display said one of said digital advertisements, and, in response to a user request, to transmit over said public packet switched communications network to at least one of said merchant computers a purchase message and to cause a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value advertised in said one of said digital advertisements and in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database;

at least one of said merchant computers being programmed to receive said purchase message, and to cause said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with purchase of said product not being a replay attack of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key.

6. An open network payment system for transferring funds having real monetary value from a sender to a beneficiary and providing for real-time authorization of payment transactions by a financial authorization network external to said network payment system, comprising:

a plurality of client computers; and

at least one payment computer;

said client computers and said payment computer being interconnected by a public packet switched communications network;

each one of said client computers being programmed to construct a payment request specifying a payment amount to be transferred from a sender to a beneficiary, and to cause said payment request to be transmitted to said payment computer over said public packet switched communications network;

said payment computer being programmed to cause a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, to receive an authorization from said financial authorization network in response to said message, to transmit an authorization message to said client computer over said public packet switched communications network, to cause information pertaining to said payment request and authorization to be recorded in a settlement database, and to cause funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an

external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signature protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key.

16. A network payment system in accordance with claim 6, wherein said payment computer is programmed to determine whether real-time authorization is necessary and to cause said message to be transmitted into said financial authorization network to verify that said sender has adequate funds or credit only if said payment computer has determined that real-time authorization is necessary.

18. A method of effecting sales over a network sales system comprising a plurality of buyer computers and a plurality of merchant computers interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions and comprising the steps of:

storing digital advertisements in a database;

receiving a user inquiry at one of said buyer computers and, in response to said user inquiry, selecting one of said merchant computers, and transmitting a network request from said one of said buyer computers thereto over said public packet switched communications network;

communicating one of said digital advertisements from one of said merchant computers to said one of said buyer computers over said public packet switched communications network in response to said network request from said buyer computer;

displaying said one of said digital advertisements at said one of said buyer computers, and, in response to a user request, transmitting over said public packet switched communications network from said one of said buyer computers to one of said merchant computers a purchase message, and causing a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value advertised in said one of said digital advertisements and in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database; and

receiving said purchase message at one of said merchant computers, and causing said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with said purchase transaction not being a replay of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from

said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key.

24. A method of transferring funds having real monetary value from a sender to a beneficiary using a network payment system comprising a plurality of client computers and at least one payment computer interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions by a financial authorization network external to said public packet switched communications network, and comprising the steps of:

constructing a payment request at one of said client computers specifying a payment amount to be transferred from a sender to a beneficiary, and causing said payment request to be transmitted to said payment computer over said public packet switched communications network; and

causing a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, receiving, at said payment computer, an authorization from said financial authorization system in response to said message, transmitting an authorization message from said payment computer to said client computer over said public packet switched communications network, causing information pertaining to said payment request and authorization to be recorded in a settlement database, and causing funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization system external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key.

38. An open network sales system providing for real-time authorization of purchase transactions, comprising:

a plurality of buyer computers; and

a plurality of merchant computers;

said plurality of buyer computers and said plurality of merchant computers being interconnected by a public packet switched communications network;

each of said buyer computers being programmed to transmit over said public packet switched communications network to at least one of said merchant computers, in response to a user request, a purchase message and to cause a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value and

in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database;

at least one of said merchant computers being programmed to receive said purchase message, and to cause said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with purchase of said product not being a replay of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key.

39. A method of effecting sales over a network sales system comprising a plurality of buyer computers and a plurality of merchant computers interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions and comprising the steps of:

in response to a user request, transmitting over said public packet switched communications network from one of said buyer computers to one of said merchant computers a purchase message, and causing a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value and in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database; and

receiving said purchase message at one of said merchant computers, and causing said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with said purchase transaction not being a replay of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key.

43. An open network payment system for transferring funds having real monetary value from a sender to a beneficiary and providing for real-time authorization of payment transactions by a financial authorization network external to said network payment system, comprising:

a plurality of client computers; and

at least one payment computer;

said client computers and said payment computer being interconnected by a public packet switched communications network;

each one of said client computers being programmed to construct a payment request specifying a payment amount to be transferred from a sender to a beneficiary, and to cause said payment request to be transmitted to said payment computer over said public packet switched communications network;

said payment computer being programmed to cause a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, to receive an authorization from said financial authorization network in response to said message, to transmit an authorization message to said client computer over said public packet switched communications network, to cause information pertaining to said payment request and said authorization to be recorded in a settlement database, and to cause funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key;

said authorization message comprising an authenticator proving that said payment computer originated said authorization message and being capable of validation without use of a secret key.

44. A method of transferring funds having real monetary value from a sender to a beneficiary using a network payment system comprising a plurality of client computers and at least one payment computer interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions by a financial authorization network external to said public packet switched communications network, and comprising the steps of:

constructing a payment request at one of said client computers specifying a payment amount to be transferred from a sender to a beneficiary, and causing said payment request to be transmitted to said payment computer over said public packet switched communications network; and

causing a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, receiving, at said payment computer, an authorization from said financial authorization system in response to said message, transmitting an authorization message from said payment computer to said client computer over said public packet switched communications network, causing information pertaining to said payment request and said authorization to be recorded in a settlement database, and causing funds having real monetary value to be

transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization system external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key;

said authorization message comprising an authenticator proving that said payment computer originated said authorization message and being capable of validation without use of a secret key.

45. A payment computer for use in transferring funds having real monetary value from a sender to a beneficiary, said payment computer being programmed to receive, over a public packet switched communications network, a payment request specifying a payment amount to be transferred from said sender to said beneficiary, said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key, said payment computer further being programmed to authenticate said payment request, to cause a message to be transmitted into a financial authorization network external to said network payment system, in order to verify that said sender has adequate funds or credit having real monetary value, to receive an authorization from said financial authorization network in response to said message, to transmit an authorization message over said public packet switched communications network, said authorization message comprising an authenticator proving that said payment computer originated said authorization message, to cause information pertaining to said payment request and authorization to be recorded in a settlement database, and to cause funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network.

46. A payment computer for use in transferring funds having real monetary value from a sender to a beneficiary, said payment computer being programmed to receive, over a public packet switched communications network, a payment request specifying a payment amount to be transferred from said sender to said beneficiary, said payment request comprising at least one digital signature of components that include components derived from said payment request, at least one of which digital signatures protects said payment request from forgery, including authenticating an identity of one of a plurality of principals as an originator of said payment request, at least one of which digital signatures protects said payment request from replay attack, and at least one of which digital signatures is computed based on a principal-specific secret key, said payment computer further being programmed to authenticate said payment request, to cause a message to be transmitted into a financial authorization network external to said network payment system, in order to verify that said sender has adequate funds or credit having

real monetary value, to receive an authorization from said financial authorization network in response to said message, to transmit an authorization message over said public packet switched communications network, said authorization message comprising an authenticator proving that said payment computer originated said authorization message and being capable of validation without use of a secret key, to cause information pertaining to said payment request and authorization to be recorded in a settlement database, and to cause funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network.

49. An open network sales system providing for real-time authorization of purchase transactions, comprising:

a plurality of buyer computers; and

a plurality of merchant computers;

said plurality of buyer computers and said plurality of merchant computers being interconnected by a public packet switched communications network;

at least one of said plurality of merchant computers being programmed to store digital advertisements in a database;

each one of said buyer computers being programmed to receive a user inquiry and, in response to said user inquiry, to select at least one of said merchant computers and to transmit a network request thereto over said public packet switched communications network;

at least one of said merchant computers being programmed to cause one of said digital advertisements to be communicated to said one of said buyer computers over said public packet switched communications network in response to said network request from said buyer computer;

said one of said buyer computers being programmed to display said one of said digital advertisements, and, in response to a user request, to transmit over said public packet switched communications network to at least one of said merchant computers a purchase message and to cause a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value advertised in said one of said digital advertisements and in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database;

at least one of said merchant computers being programmed to receive said purchase message, and to cause said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network as evidenced by a payment response from said payment system, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with purchase of said product not being a replay attack of a message previously transmitted over said

public packet switched communications network;

said payment response comprising at least one digital signature of components that include components derived from said payment response, at least one of which digital signatures protects said payment response from forgery, including authenticating an identity of a source as an originator of said payment response, at least one of which digital signatures protects said payment response from replay attack, and at least one of which digital signatures is computed based on a source-specific secret key.

50. An open network payment system for transferring funds having real monetary value from a sender to a beneficiary and providing for real-time authorization of payment transactions by a financial authorization network external to said network payment system, comprising:

a plurality of client computers; and

at least one payment computer;

said client computers and said payment computer being interconnected by a public packet switched communications network;

each one of said client computers being programmed to construct a payment request specifying a payment amount to be transferred from a sender to a beneficiary, and to cause said payment request to be transmitted to said payment computer over said public packet switched communications network;

said payment computer being programmed to cause a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, to receive an authorization from said financial authorization network in response to said message, to transmit an authorization message to said client computer over said public packet switched communications network, to cause information pertaining to said payment request and authorization to be recorded in a settlement database, and to cause funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said authorization message comprising at least one digital signature of components that include components derived from said authorization message, at least one of which digital signatures protects said authorization message from forgery, including authenticating an identity of a source as an originator of said authorization message, at least one of which digital signatures protects said authorization message from replay attack, and at least one of which digital signatures is computed based on a source-specific secret key.

51. A method of effecting sales over a network sales system comprising a plurality of buyer computers and a plurality of merchant computers interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions and comprising the steps of:

storing digital advertisements in a database;

receiving a user inquiry at one of said buyer computers and, in response to said user inquiry, selecting one of said merchant computers, and transmitting a network request from said one of said buyer computers thereto over said public packet switched communications network;

communicating one of said digital advertisements from one of said merchant computers to said one of said buyer computers over said public packet switched communications network in response to said network request from said buyer computer;

displaying said one of said digital advertisements at said one of said buyer computers, and, in response to a user request, transmitting over said public packet switched communications network from said one of said buyer computers to one of said merchant computers a purchase message, and causing a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value advertised in said one of said digital advertisements and in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database; and

receiving said purchase message at one of said merchant computers, and causing said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network as evidenced by a payment response from said payment system, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with said purchase transaction not being a replay of a message previously transmitted over said public packet switched communications network;

said payment response comprising at least one digital signature of components that include components derived from said payment response, at least one of which digital signatures protects said payment response from forgery, including authenticating an identity of a source as an originator of said payment response, at least one of which digital signatures protects said payment response from replay attack, and at least one of which digital signatures is computed based on a source-specific secret key.

52. A method of transferring funds having real monetary value from a sender to a beneficiary using a network payment system comprising a plurality of client computers and at least one payment computer interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions by a financial authorization network external to said public packet switched communications network, and comprising the steps of:

constructing a payment request at one of said client computers specifying a payment amount to be transferred from a sender to a beneficiary, and causing said payment request to be transmitted to said payment computer over said public packet switched communications network; and

causing a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, receiving, at said payment computer, an authorization from said financial authorization system in response to said message, transmitting an authorization message from said payment computer to said client computer over said public packet switched communications network, causing information pertaining to said payment request and authorization to be recorded in a settlement database, and causing funds having real monetary value to be

transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization system external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said authorization message comprising at least one digital signature of components that include components derived from said authorization message, at least one of which digital signatures protects said authorization message from forgery, including authenticating an identity of a source as an originator of said authorization message, at least one of which digital signatures protects said authorization message from replay attack, and at least one of which digital signatures is computed based on a source-specific secret key.

53. An open network sales system providing for real-time authorization of purchase transactions, comprising:

a plurality of buyer computers; and

a plurality of merchant computers;

said plurality of buyer computers and said plurality of merchant computers being interconnected by a public packet switched communications network;

each of said buyer computers being programmed to transmit over said public packet switched communications network to at least one of said merchant computers, in response to a user request, a purchase message and to cause a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value and in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database;

at least one of said merchant computers being programmed to receive said purchase message, and to cause said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network as evidenced by a payment response from said payment system, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with purchase of said product not being a replay of a message previously transmitted over said public packet switched communications network;

said payment response comprising at least one digital signature of components that include components derived from said payment response, at least one of which digital signatures protects said payment response from forgery, including authenticating an identity of a source as an originator of said payment response, at least one of which digital signatures protects said payment response from replay attack, and at least one of which digital signatures is computed based on a source-specific secret key.

54. A method of effecting sales over a network sales system comprising a plurality of buyer computers and a plurality of merchant computers interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions and comprising the steps of:

in response to a user request, transmitting over said public packet switched communications network from one of said buyer computers to one of said merchant computers a purchase message, and causing a payment request, comprising a payment amount, to be transmitted over said public packet switched communications network into a payment system comprising a financial authorization network external to said public packet switched communications network, in order to initiate authorization of purchase of a product having real monetary value and in order to initiate recordation of information pertaining to said payment request and an authorization in a settlement database; and

receiving said purchase message at one of said merchant computers, and causing said product to be sent to a party conditioned on said purchase transaction having been authorized in real time by said financial authorization network external to said public packet switched communications network as evidenced by a payment response from said financial authorization network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to a principal making said payment, and conditioned on at least one message transmitted over said public packet switched communications network in connection with said purchase transaction not being a replay of a message previously transmitted over said public packet switched communications network;

said payment response comprising at least one digital signature of components that include components derived from said payment response, at least one of which digital signatures protects said payment response from forgery, including authenticating an identity of a source as an originator of said payment response, at least one of which digital signatures protects said payment response from replay attack, and at least one of which digital signatures is computed based on a source-specific secret key.

55. An open network payment system for transferring funds having real monetary value from a sender to a beneficiary and providing for real-time authorization of payment transactions by a financial authorization network external to said network payment system, comprising:

a plurality of client computers; and

at least one payment computer;

said client computers and said payment computer being interconnected by a public packet switched communications network;

each one of said client computers being programmed to construct a payment request specifying a payment amount to be transferred from a sender to a beneficiary, and to cause said payment request to be transmitted to said payment computer over said public packet switched communications network;

said payment computer being programmed to cause a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, to receive an authorization from said financial authorization network in response to said message, to transmit an authorization message to said client computer over said public packet switched communications network, to cause information pertaining to said payment request and said authorization to be recorded in a settlement database, and to cause funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization network external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real

monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said authorization message comprising at least one digital signature of components that include components derived from said authorization message, at least one of which digital signatures protects said authorization message from forgery, at least one of which digital signatures protects said authorization message from replay attack; and

said authorization message comprising an authenticator proving that said payment computer originated said authorization message and being capable of validation without use of a secret key.

57. A method of transferring funds having real monetary value from a sender to a beneficiary using a network payment system comprising a plurality of client computers and at least one payment computer interconnected by a public packet switched communications network, said method providing for real-time authorization of purchase transactions by a financial authorization network external to said public packet switched communications network, and comprising the steps of:

constructing a payment request at one of said client computers specifying a payment amount to be transferred from a sender to a beneficiary, and causing said payment request to be transmitted to said payment computer over said public packet switched communications network; and

causing a message to be transmitted into said financial authorization network external to said public packet switched communications network, in order to verify that said sender has adequate funds or credit having real monetary value, receiving, at said payment computer, an authorization from said financial authorization system in response to said message, transmitting an authorization message from said payment computer to said client computer over said public packet switched communications network, causing information pertaining to said payment request and said authorization to be recorded in a settlement database, and causing funds having real monetary value to be transferred from said sender to said beneficiary conditioned on said payment request having been authorized in real time by said financial authorization system external to said public packet switched communications network, based on an external credit card account or an external demand deposit account having sufficient credit or funds of real monetary value available to said sender, and conditioned on at least one message transmitted over said public packet switched communications network in connection with transfer of said funds not being a replay of a message previously transmitted over said public packet switched communications network;

said authorization message comprising at least one digital signature of components that include components derived from said authorization message, at least one of which digital signatures protects said authorization message from forgery, and at least one of which digital signatures protects said authorization message from replay attack; and

said authorization message comprising an authenticator proving that said payment computer originated said authorization message and being capable of validation without use of a secret key.